(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2005 年5 月6 日 (06.05.2005)

PCT

(10) 国際公開番号
WO 2005/041474 A1

(51) 国際特許分類[7]: H04L 9/32, 9/08, G06F 15/00

(21) 国際出願番号: PCT/JP2004/015184

(22) 国際出願日: 2004 年10 月7 日 (07.10.2004)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願 2003-367527
2003 年10 月28 日 (28.10.2003) JP

(71) 出願人 (米国を除く全ての指定国について): 財団法人生産技術研究奨励会 (THE FOUNDATION FOR THE PROMOTION OF INDUSTRIAL SCIENCE) [JP/JP]; 〒153-8505 東京都 目黒区 駒場４－６－１ Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 今井 秀樹 (IMAI,Hideki) [JP/JP]; 〒244-0801 神奈川県 横浜市 戸塚区品濃町５５７－４４－２０５ Kanagawa (JP). 古原 和邦 (KOBARA,Kazukuni) [JP/JP]; 〒181-0015 東京都 三鷹市 大沢２－２０－３１－１－４０２ Tokyo (JP). 辛 星漢 (SHIN,Seonghan) [KR/JP]; 〒153-8505 東京都 目黒区 駒場４－６－１ 東京大学生産技術研究所内 Tokyo (JP).

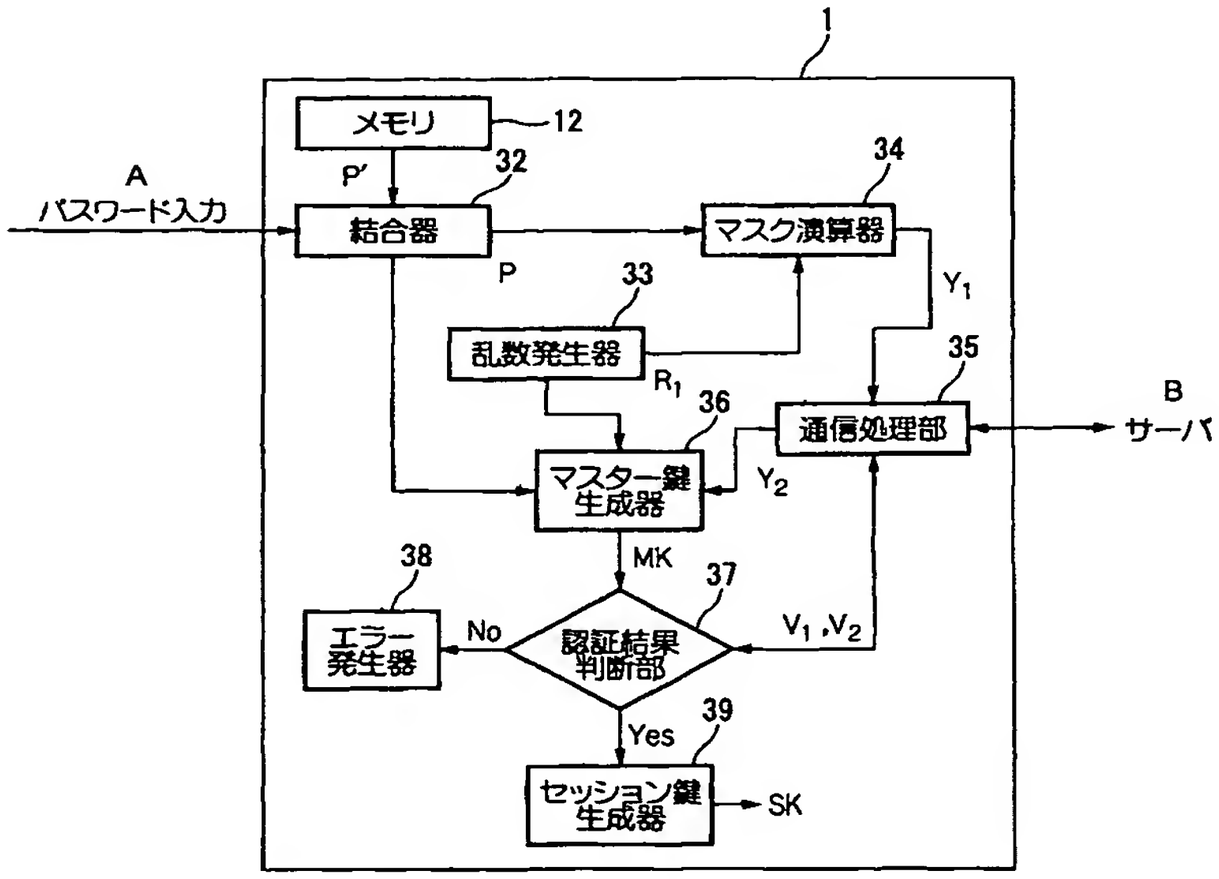
(74) 代理人: 志賀 正武, 外(SHIGA,Masatake et al.); 〒104-8453 東京都 中央区 八重洲２丁目３番１号 Tokyo (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR,

[続葉有]

(54) Title: AUTHENTICATION SYSTEM, AND REMOTELY DISTRIBUTED STORAGE SYSTEM

(54) 発明の名称: 認証システム及び遠隔分散保存システム



A... INPUT PASSWORD
12... MEMORY
32... COUPLER
34... MASK ARITHMETIC UNIT
33... RANDOM NUMBER GENERATOR
35... COMMUNICATION PROCESSING PART
B... SERVER
36... MASTER KEY GENERATOR
38... ERROR GENERATOR
37... AUTHENTICATION RESULT JUDGING PART
39... SESSION KEY GENERATOR

(57) Abstract: An authentication system wherein a terminal apparatus (1) uses a master key generator (36) to generate, based on an input password and a predetermined calculation, a value MK, and further uses an authentication result judging part (37) to calculate, from the value MK, values V1 and V2, and wherein the terminal apparatus (1) transmits the value V1 to a server (2). The server (2) uses a master key generator (45) to generates, based on a password of server registration of the terminal apparatus (1) shared and stored in advance through safe communication means and based on a predetermined calculation, a value MK, and further uses an authentication result judging part (46) to calculate, from the value MK, values V1 and V2. The server (2) transmits the value V2 to the terminal apparatus (1). Mutual authentications are performed dependently on whether these values can be calculated based on the predetermined calculations.

[続葉有]

WO 2005/041474 A1

BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(57) 要約:

端末装置１は入力されたパスワードに基づいて所定計算によりマスター鍵生成器３６で生成した値ＭＫから認証結果判断部３７にて値Ｖ１，Ｖ２を計算してサーバ２に値Ｖ１を送信し、前記サーバ２は安全な通信手段により予め共有し記録しておいた前記端末装置１のサーバ登録用のパスワードに基づいて所定計算によりマスター鍵生成器４５で生成した値ＭＫから認証結果判断部４６にて値Ｖ１，Ｖ２を計算して前記端末装置１に値Ｖ２を送信し、これら値が所定計算により算出できるか否かにより相互の認証を行う認証システム。